SE2 Insures Itself Against Advanced Threats

Proactive Protection for Clients' Sensitive Financial Data and Simplified Security Management with Check Point SandBlast

"CPU-level inspection makes SandBlast even more attractive. It prevents exploits like Return-Oriented Programming attacks, and the sandboxing process is fast. Speed, simplicity, and ease of use mean a lot to us."

— Saul Schwartz, Enterprise Security Engineer, SE2

Customer Profile

SE2 is a third party administration services provider to major insurance carriers around the globe.

Challenge

- Protect clients' highly sensitive financial data from being leaked, exfiltrated, or held for ransom
- Proactively prevent unknown malware and zero-day threats,

Solution

- Check Point SandBlast Zero-Day Protection

Benefits

- Prevents unknown threats and dangerous exploits from gaining access
- Increased visibility into threats with detailed reporting
- Simplified management by consolidating everything under a single pane of glass

Overview

SE2

Headquartered in Topeka, Kansas, SE2 provides third party administration services to life and annuity insurance carriers, helping them launch products rapidly, improve efficiencies and maximize profits while improving the customers' experience and enabling a shift to a variable cost model.

Business Challenge

There Has to be a Better Way

Insurance carriers maintain large stores of sensitive client information, financial data, and proprietary analysis information. But as competition increases, many carriers are turning to third party administrators (TPAs) to reduce costs, improve customer service, and become more agile.

"We're definitely growing," said Saul Schwartz, Enterprise Security Engineer at SE2. "As our customer base grows, so does the amount of sensitive financial data that we have to protect. We're responsible for multiple carriers' business-critical data, so defending it is a top priority."

Keeping up with new threats was a constant challenge, consuming a significant portion of the security team's time. Every day they monitored logs, reviewed events, and simultaneously tried to advance new security projects. But it never seemed to be enough. Schwartz was spending tens of hours every week triaging alerts and instructing technicians on virus and malware remediation. SE2 had an existing sandboxing solution, but it took up to 10 minutes to alert the team after malware hit a workstation. By then, it was too late to stop, resulting in additional effort to remediate any impact.

"I don't want to have to explain to my CIO that we've just had a million life insurance policies made inaccessible by cryptolocker," said Schwartz. "That's one of my biggest concerns. And it's why I began looking for a better threat emulation (sandboxing) solution."

Schwartz's list of requirements included faster emulation—as close to real time as possible. He wanted a way to block threats, instead of just alerting him after the fact. He also wanted to consolidate everything to a single pane of glass, eliminating the need to manage multiple appliances and policies. List in hand, he and his team began evaluating alternative solutions.

"We checked with our compliance team to see if we could operate SandBlast in the cloud, and they had no restrictions. It was so simple to activate using our existing Check Point gateway. We literally activated a license and turned it on."

— Saul Schwartz,
Enterprise Security Engineer, SE2

Solution

A Simple Ounce of Prevention

The security team tried several solutions, including Check Point SandBlast. To compare them, Schwartz ran the solutions simultaneously in detect mode. In just one week, the competitive appliance missed several instances and failed to alert Schwartz, but SandBlast caught all of them.

"We checked with our compliance team to see if we could operate SandBlast in the cloud, and they had no restrictions," said Schwartz. "It was so simple to activate using our existing Check Point gateway. We literally activated a license and turned it on."

With SandBlast zero-day protection deployed, Schwartz gained superb threat prevention capabilities. He no longer has to spend time tracking down alerts, because machines are not being infected, and he rarely has to activate the incident response plan anymore.

"Consolidating everything under a single pane of glass has been a big help. Check Point SandBlast not only delivers better protection,it greatly simplifies a large portion of our enterprise security operations."

— Saul Schwartz,
Enterprise Security Engineer, SE2

Benefits

Great Detection, Even Better Prevention

"I was afraid that SandBlast would flag some of our legacy application traffic, because it's older and might appear suspicious, but it didn't," said Schwartz. "It caught legitimate malware and infections that otherwise would have slipped through the cracks. It catches 20 to 30 attacks per week from web browsing alone."

SandBlast Threat Emulation uses OS-level inspection to examine a wide range of file types and catch threats before they are deployed. In addition, patented deep CPU-level inspection stops even the most dangerous attacks before they can escape detection. With SandBlast, Schwartz achieved his goal of preventing infections and attacks.

"CPU-level inspection makes SandBlast even more attractive," he said. "It prevents exploits like Return-Oriented Programming attacks, and the sandboxing process is fast. The speed, simplicity, and ease of use mean a lot to us."

Clearer, Centralized Visibility

SandBlast also gives Schwartz the centralization and visibility he needs. With the SmartLog and SmartView Tracker on their Check Point firewall, Schwartz can filter and see all traffic and malware that SandBlast is preventing. The team can dive into the sandbox analysis capability and see specific details—such as screenshots of what was opened, registry keys, and malware command-and-control addresses.

"Consolidating everything under a single pane of glass has been a big help," said Schwartz. "Check Point SandBlast not only delivers better protection, it greatly simplifies a large portion of our enterprise security operations."

For more information, visit
www.checkpoint.com/sandblast